CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

DIEGO ANDRÉS BELTRÁN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD JOSE ACEVEDO Y GOMEZ - BOGOTÁ
2021

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

DIEGO ANDRÉS BELTRÁN PARRA

DIRECTOR DE SEMINARIO: JOHN FREDDY QUINTERO TAMAYO
M.Sc.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD JOSE ACEVEDO Y GOMEZ - BOGOTÁ

2021

RESUMEN

De acuerdo a las actividades realizadas dentro del seminario de especialización equipos RedTeam & BlueTeam se consolida un informe técnico que permite evidenciar cada punto importante y sus escenarios presentados, permitiendo abordar los diferentes aspectos tanto éticos como legales además de la explicación puntual de los métodos, técnicas y herramientas usadas demostrando las capacidades de cada equipo y su adecuada intervención. Finalmente se encuentra un desgloce de información importante tomado del framework NIST para las buenas practicas de ciberseguridad y los lineamientos estrategicos.

Cada aspecto se convierte en lineamientos base para tener en cuenta, implementar y referenciar al momento de presentar situaciones similares entorno a reacciones de equipos de ataque y defensa además de contar con el personal calificado que pueda operar las diferentes herramientas y plantear un análisis profesional de acuerdo al escenario.

TABLA DE CONTENIDO

Pág.

TABLA DE ILUSTRACIONES

Pág.

1. INTRODUCCIÓN

A partir de este documento, permitirá identificar y evaluar las acciones de los equipos Red Team & Blue Team de una organización. Demostrar bajo escenario propuesto las diferentes vulnerabilidades y acceso a los sistemas de información de una maquina afectada. A su vez generar conciencia y establecer lineamientos de protección y prevención sobre estas actividades.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

2.2. OBJETIVOS ESPECÍFICOS

- Construir informe técnico, el cual refleja el desarrollo de las actividades del curso presentado consistencia entre: título, objetivos, desarrollo del informe, conclusiones y recomendaciones
- Presentar conclusiones donde se señale la importancia de desplegar estrategias relacionadas con RedTeam & BlueTeam.
- Presentar recomendaciones donde se plantea estrategias para contribuir en la mejora de técnicas para RedTeam & BlueTeam.

3. DESARROLLO DEL INFORME TÉCNICO

A continuación se relacionan los escenarios expuestos durante el seminario.
Estado Análisis ético y legal al acuerdo de confidencialidad con whitehouse security

Fecha de descubrimiento 10/03/2021
Activo 1 Acuerdo de confidencialidad con whitehouse security
Criticidad Alta
Impacto 7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Categoría Documentación
Prueba Manual
Código CWE-200
Plataforma Texto
DESCRIPCIÓN
El primer aspecto es conocer la ley 1273 de 2009[1] e identificar en que articulos de dicha ley Irrumpe.

Explotación / Descubrimiento
Para tal efecto, por lo anterior y dando enfasis a la ley 1273 de 2009 el contrato (Anexo 3 - Acuerdo) Irrumpe en los articulos:

Capitulo Primero

Artículo 369A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO
Artículo 269B. OBSTACULIZACIÓN ILEGITIMA DEL SISTEMA INFORMÁTICO
Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS
Artículo 269F. VIOLACIÓN DE DATOS PERSONALES
Artículo 269H. CIRCUNSTANCIAS DE AGRAVACiÓN PUNITIVA punto 7: Utilizando como instrumento a un tercero de buena fe

Capitulo Segundo

ARTÍCULO 269J TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

[1] MinTic Colombia. Ley 1273 de 2009, consultado en https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf enlace activo al 20/02/2021

Los procesos poco confiables y de dudosa reputación dan por entendido que se trata de una organización delincuencial atañando temas legales por contrato y responsablilidad a quien acordarse y firmase sin leer previamente dicho acuerdo, quizá en su mayoría por tentativa de remuneración económica (en este caso $15.000.000). De acuerdo a la Ley 1273 del 5 de enero de 2009 para el ciber delincuente aplicarían sanciones bajo los artículos anteriormente mencionados (Congreso de Colombia, 2009)

El segundo aspecto es conocer el código de ética para el ejercicio de la ingeniería en general impartido por el copnia.

Por lo tanto y basado en el profesionalismo y la responsabilidad consignada en el codigo de ética profesional impartido por el COPNIA[2] y la Ley 842 de 2003 se hace enfásis en:
Capitulo I.
Artículo 29 POSTULADOS ÉTICOS DEL EJERCICIO PROFESIONAL

Capitulo II.
Artículo 31 DEBERES GENERALES DE LOS PROFESIONALES. sección F: Denunciar los delitos, contravenciones y faltas contra el código.

Artículo 32 PROHIBICIONES GENERALES A LOS PROFESIONALES. sección B: Permitir, tolerar o facilitar el ejercicio ilegal.

Como lo asocia el el Anexo 3 - Acuerdo del contrato al igual que la sección K: Participar en licitaciones, concursar o suscribir contratos estatales.

Haciendo uso del Artículo 33 Como DEBERES ESPECIALES DE LOS PROFESIONALES PARA CON LA SOCIEDAD. En la sección E: Rechazar toda clase de trabajos que en este caso implicarán daños evitables para la sociedad.

Enfocando en la firma de los contratos se evita incumplir en todo el Artículo 34 PROHIBICIONES ESPECIALES A LOS PROFESIONALES y el Artículo 37-38 DEBERES DE LOS PROFESIONALES PARA CON SUS COLEGAS Y DEMÁS PROFESIONALES.

[2]COPNIA, Código de ética para el ejercicio en general y sus profesiones afinse y auxiliares. Tomado de https://www.copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf enlace activo al 20/02/2021

- Análisis del caso “operación andromeda buggly”

Haciendo un énfasis en las actividades que se realizaron y de acuerdo a las normas tanto del codigo de ética profesional y la ley 1273 de 2009 podemos observar la vulneración de los siguientes artículos:

- ✓ Como lo menciona la ley 1273 de 2009 en los artículos 269A Acceso abusivo a un sistema informático. Cuando acceden ilegalmente a los telefonos y correos electónicos o computadoras.
- ✓ Artículo 269C Interceptación de datos informáticos. Cuando interceptan comunicaciones de chat o WhatsApp, interceptación de cuentas de correo.
- ✓ Artículo 269D Daño Informático. Cuando eliminan las evidencias realizando borrados seguros a los discos duros y sacando todo lo de ciberguerra de Andromeda.
- ✓ Artículo 269F Violación de Datos personales. De acuerdo a la ley 1581 de 2012 se observa violación de datos obtenidos mediante los diferentes medios ilicitos de interceptación y acceso abusivo.
- ✓ Para los reclutadores o empresa fachada también se aplica el artículo 269J. del capitulo II Transferencia no consentida de activos, esto en los contratos y en el software utilizado.
- ✓ Por parte de los deberes como profesionales, basados en la identidad confirmada de algunos ingenieros, se aplica el código de ética el cual, por revelar información confidencial, usar la profesión de ingeniero para cometer actos ilícitos, la falta de honestidad en los procesos, obstaculización de investigaciones, actuar de manera lucrativa o ambición de dinero entre otros, de inmediato se le será suspendida la matricula profesional.

Estado Banco de trabajo, Explotación y Contención de ataques informáticos

Fecha de descubrimiento 10/03/2021
Activo 1 Windows 7 X64 IP 10.0.2.16
Criticidad Alta
Impacto 7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Categoría Aplicación
Prueba Manual
Código CWE-200
Plataforma Local

DESCRIPCIÓN

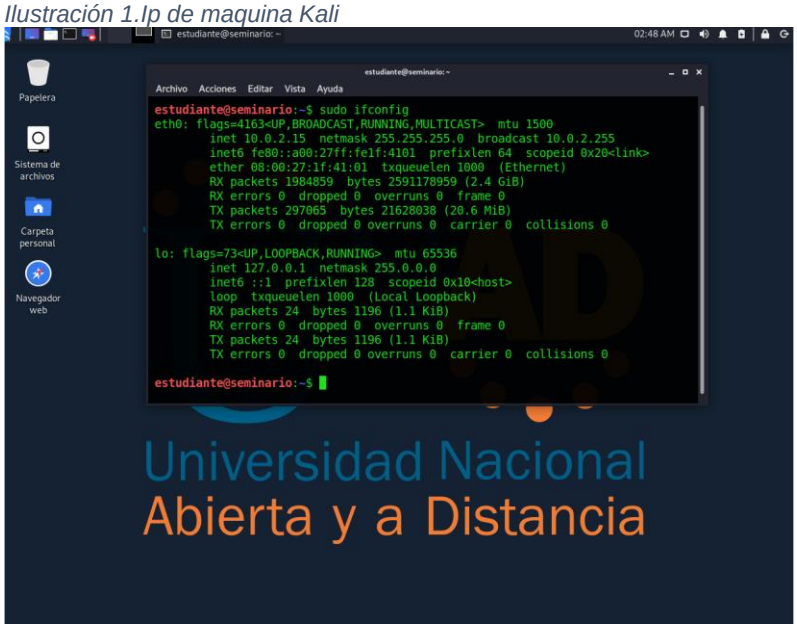
Se procedió a identificar y Se realizar pruebas de caja blanca de acuerdo a que se cuenta con credenciales de acceso, la revisión de seguridad se centra puntualmente en los accesos transversales para la máquina Windows 7 X64, dando alcance desde el 01 de febrero a las 00:00 horas hasta el 4 de abril del 2021 a las 23:55 horas.

Identificación del banco de trabajo

- CARACTERÍSTICAS TÉCNICAS

Kali Linux:
Memoria ram base: 2048 MB
IP: 10.0.2.15
BROADCAST: 10.0.2.255

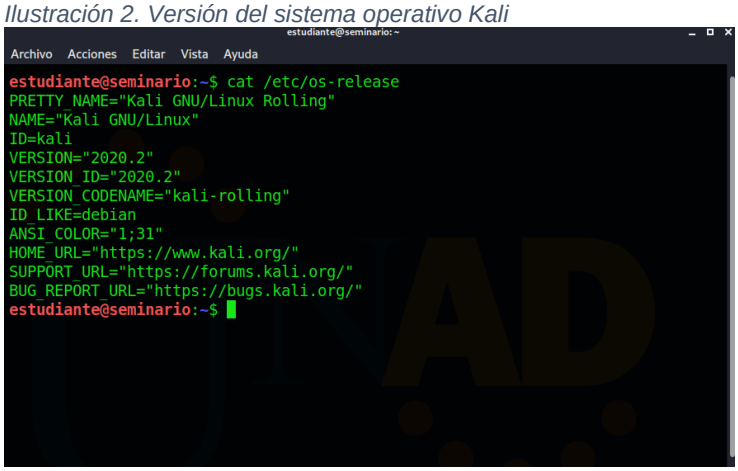
Ilustración 1.Ip de maquina Kali



Fuente: Propia de la actividad

Se observa la IP de la maquina Kali Linux la cual se obtiene con el comando ifconfig

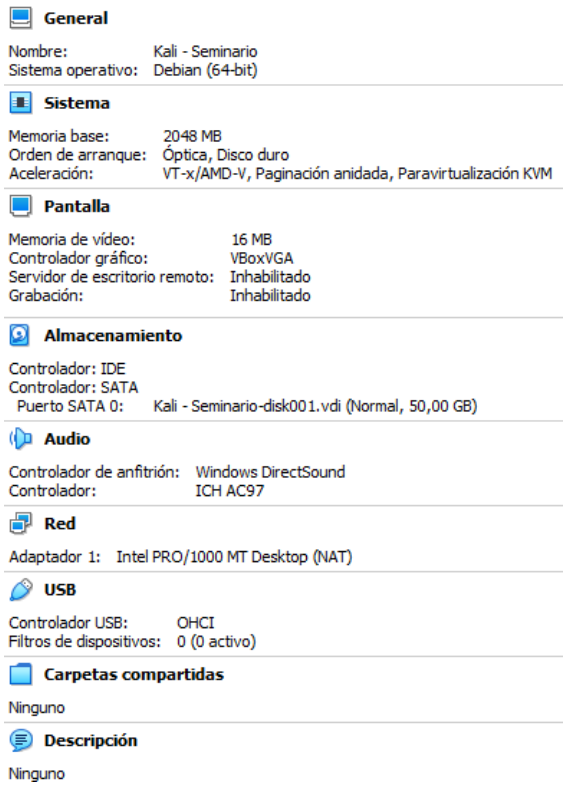
Ilustración 2. Versión del sistema operativo Kali



Fuente: Propia de la actividad

Se obtiene la versión del sistema operativo kali linux con el comando cat /etc/os-release

Ilustración 3. Generalidades desde VirtualBox para la maquina Kali

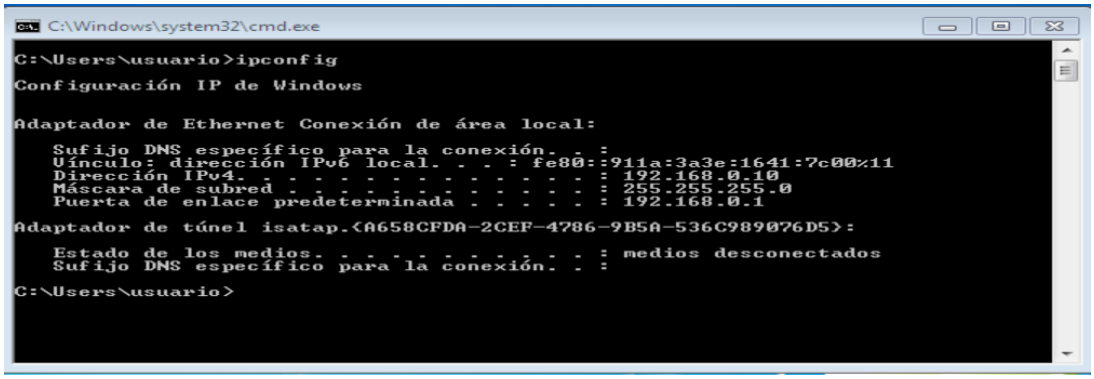


Fuente: Propia de la actividad

Información disponible de las caracteristicas de la maquina virtual Kali - Seminario desde virtualbox

Windows 7 X32
Memoria base: 4096 MB
IP: 192.168.0.10
PUERTA DE ENLACE: 192.168.0.1

Ilustración 4. Ip de la maquina Windows 7 X32



Fuente: Propia de la actividad

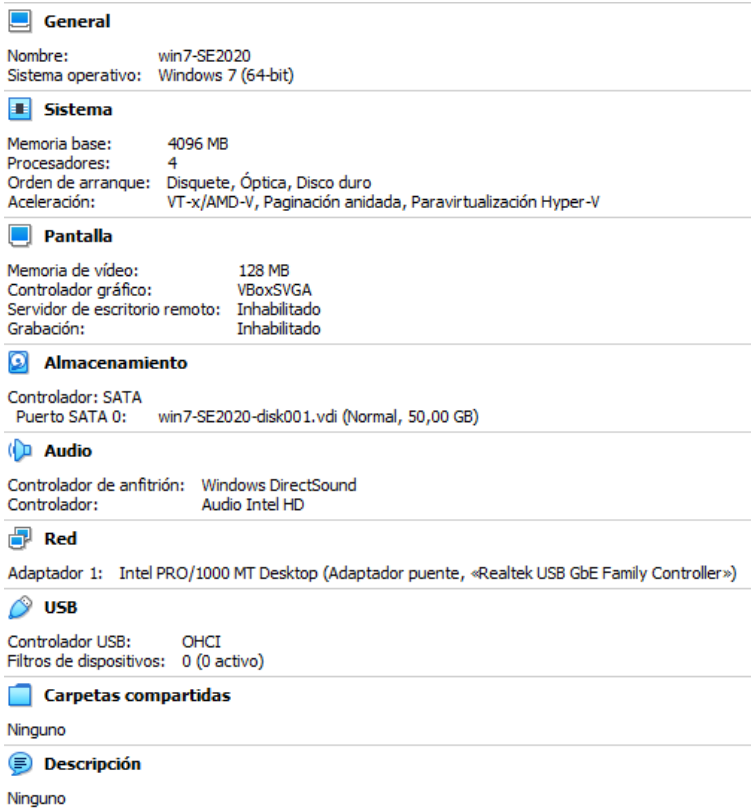
Extracción de la IP en la maquina Windows 7 X32 con el comando ipconfig

Ilustración 5. Información del sistema operativo Win7 X32 y versión

Fuente: Propia de la actividad

Información de la maquina Windows 7 X32 extraida con el comando systeminfo desde la consola

Ilustración 6. Información de VirtualBox para la maquina win7-X32



Fuente: Propia de la actividad

Información disponible de las caracteristicas de la maquina virtual Widnows 7 X32 desde virtualbox

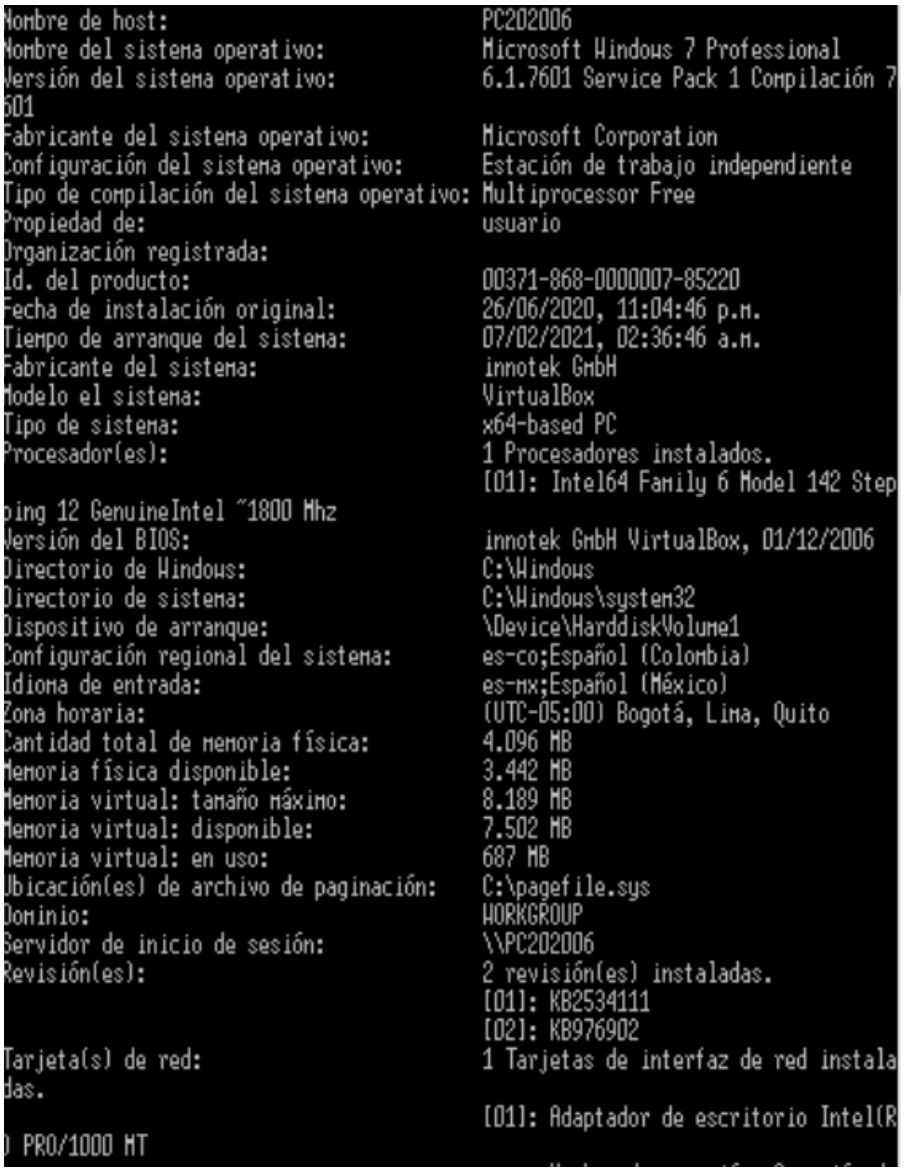
Windows 7 X64
Memoria base 4096 MB
IP: 10.0.2.16
PUERTA DE ENLACE: 10.0.2.2

Ilustración 7. Ip de la maquina Windows 7 X64

Fuente: Propia de la actividad

Información de la maquina:

Ilustración 8. Información del sistema operativo Win7 X64 y versión



Fuente: Propia de la actividad

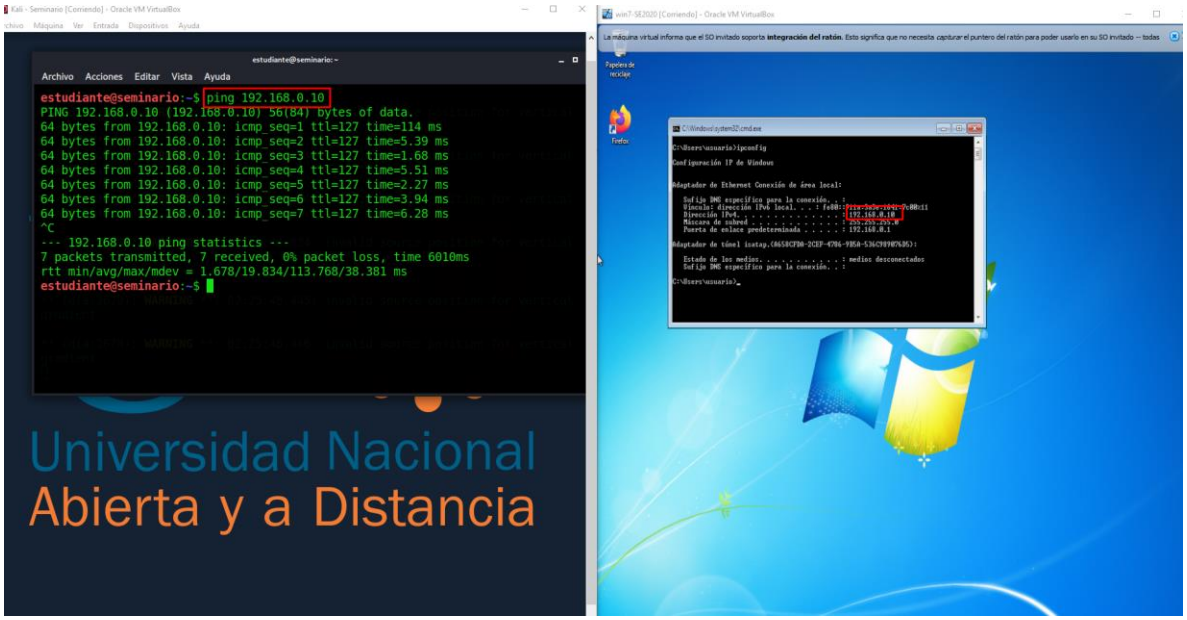
Información de la maquina Windows 7 X64 extraida con el comando systeminfo desde la consola

Ilustración 9. Información de VirtualBox para la maquina win7-X64

Fuente: Propia de la actividad

Información disponible de las caracteristicas de la maquina virtual Windows 7 X64 desde virtualbox

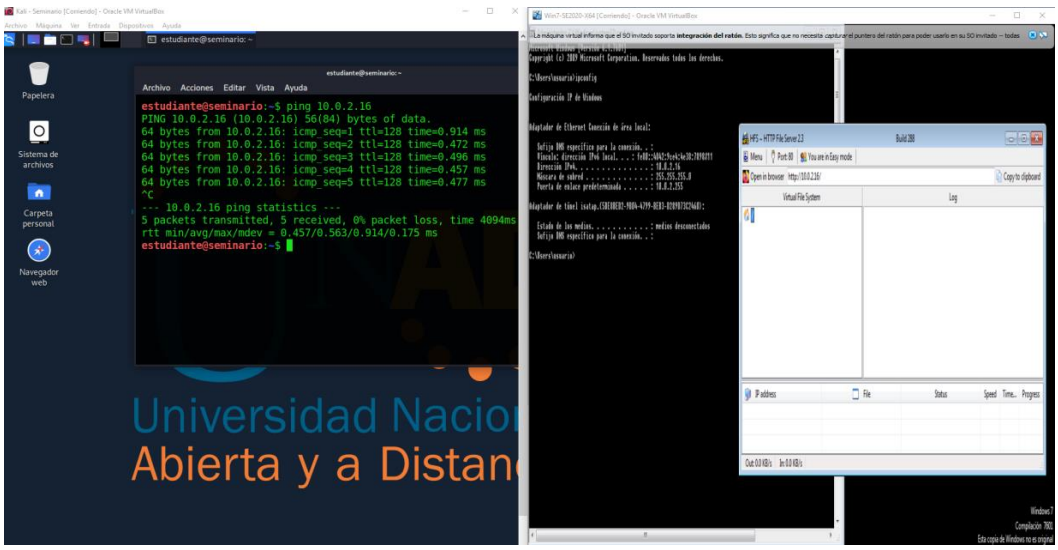
Ilustración 10. Ping de Kali a Windows 7 X32



Fuente: Propia de la actividad

Comunicación entre Kali linux y Win7-SE2020 veriricación con un ping sostenido

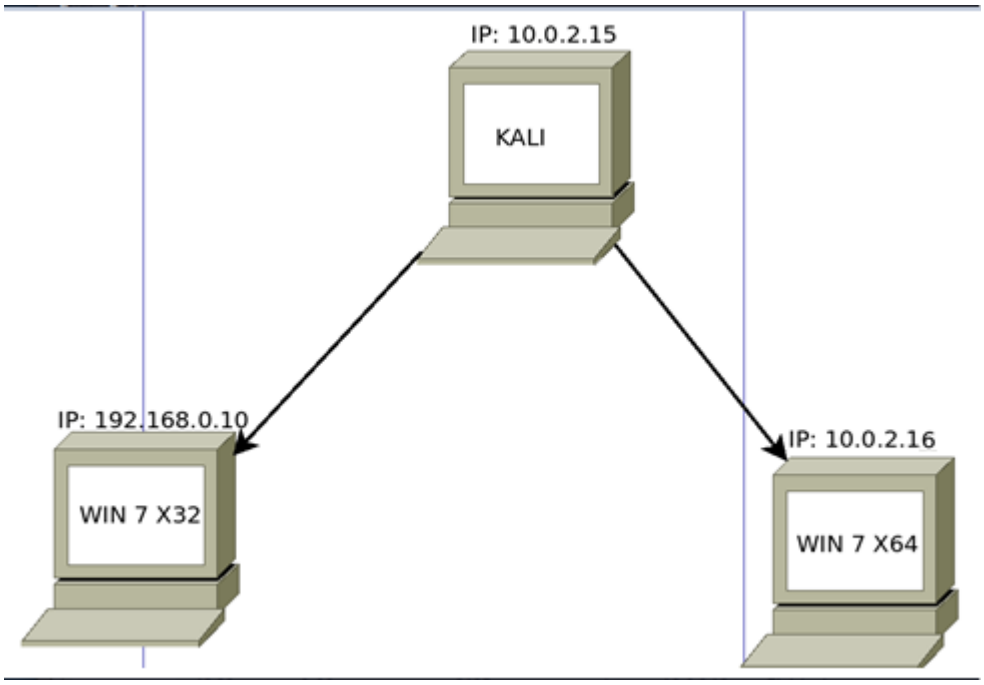
Ilustración 11. Ping de Kali a Windows 7 X64



Fuente: Propia de la actividad

Comunicación entre Kali linux y Win7-X64 veriricación con un ping sostenido

Ilustración 12. Diagrama de red del escenario propuesto



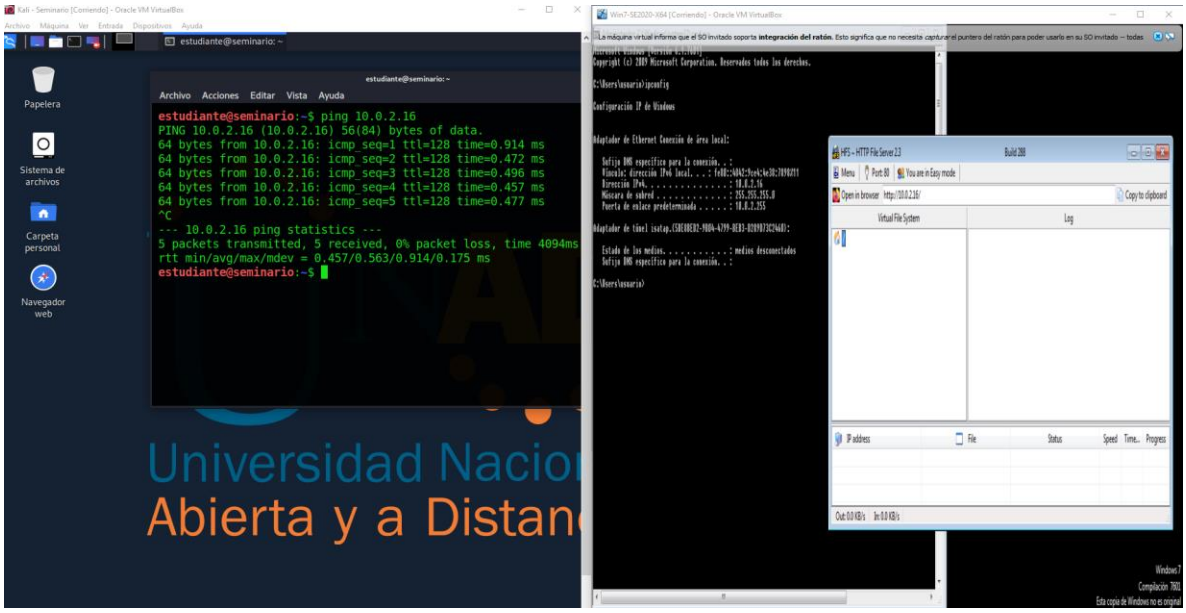
Fuente: Propia de la actividad

Diagrama de red en el cual se visualiza una maquina principal (Kali linux) con la que se muestra comunicación desde kali linux a ambas maquinas windows

Seguido se procedió a identificar y explotar las vulnerabilidades existentes en la maquina objetivo Windows7 X64.

- EXPLOTACIÓN DE VULNERABILIDADES DETECTADAS

Ilustración 13. Reconocimiento de maquima victima

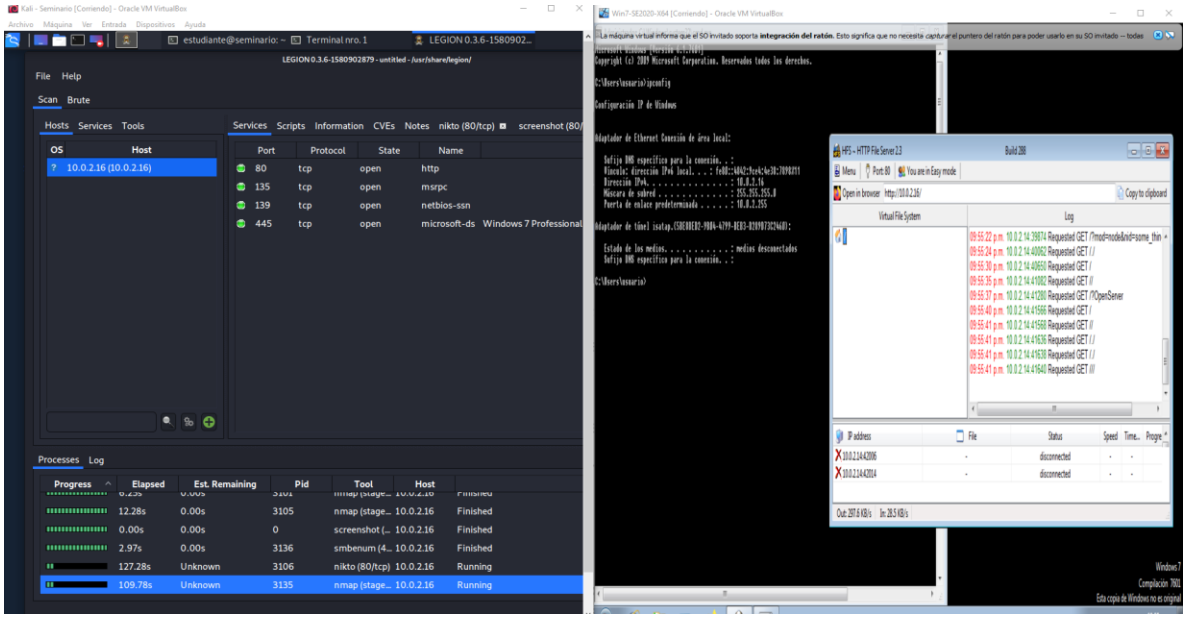


Fuente: Propia de la actividad

De acuerdo a la metodología OWASAP se procede a adoptar y aplicar los diferentes pasos para la obtención y explotación de las diferentes pruebas de intrusión.

1. Levantamiento de información con Legión

Ilustración 14. Enumeración de puertos con Legión



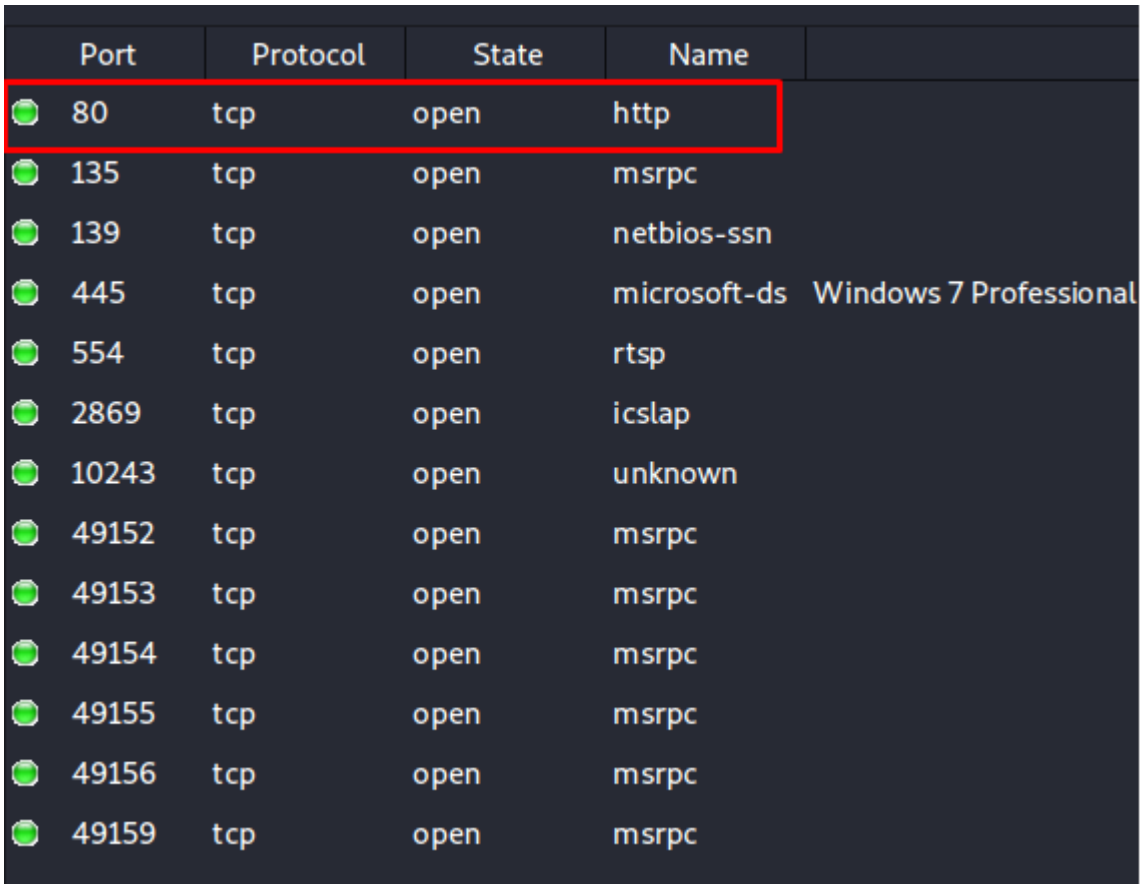
Fuente: Propia de la actividad

Se procede a automarizar el proceso de apertura de puertos entre otros con la herramienta Legión que viene con Kali Linux.

Como tal el HFS registra las peticiones realizadas por legión desde kali

2. Enumeración

Ilustración 15. Puerto usado por HFS.

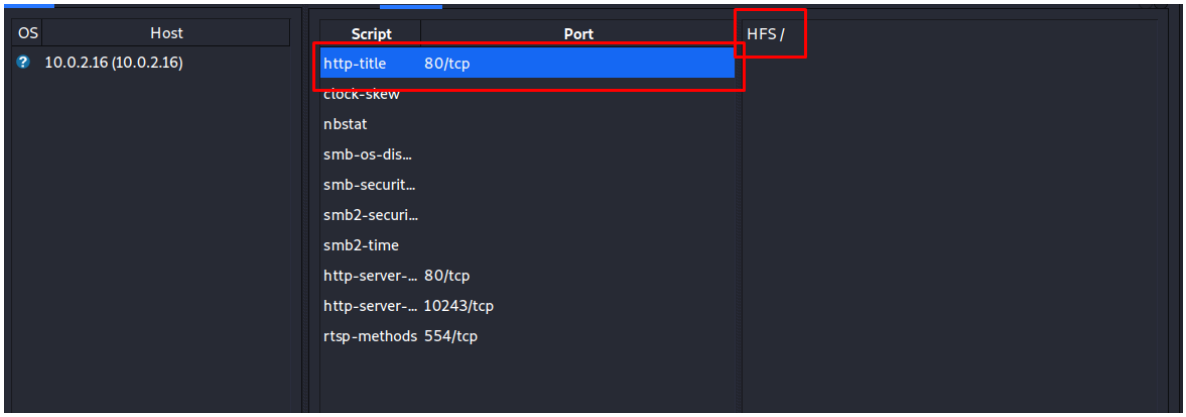


Port	Protocol	State	Name	
80	tcp	open	http	
135	tcp	open	msrpc	
139	tcp	open	netbios-ssn	
445	tcp	open	microsoft-ds	Windows 7 Professional
554	tcp	open	rtsp	
2869	tcp	open	icslap	
10243	tcp	open	unknown	
49152	tcp	open	msrpc	
49153	tcp	open	msrpc	
49154	tcp	open	msrpc	
49155	tcp	open	msrpc	
49156	tcp	open	msrpc	
49159	tcp	open	msrpc	

Fuente: Propia de la actividad

Se identifica el puerto que el HFS tiene habilitado en este caso el puerto 80

Ilustración 16. Identificación de Servicio



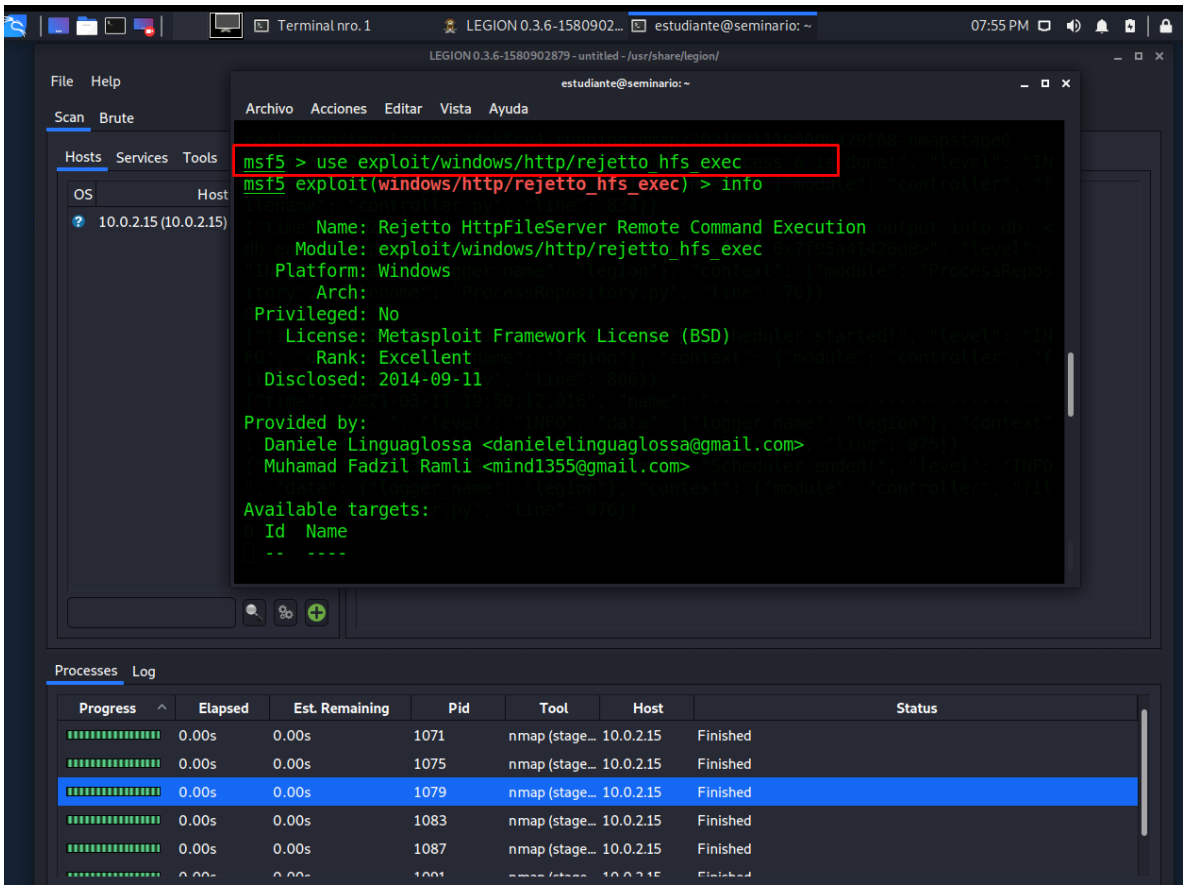
Fuente: Propia de la actividad

Se identifica con Legión el servicio que se está ejecutando desde el puerto 80 de la maquina Windows 7 X64 y se observa que es HFS

Una vez realizada la enumeración e identificación de servicios vulnerables se procede a realizar el respectivo ataque

3. Explotación

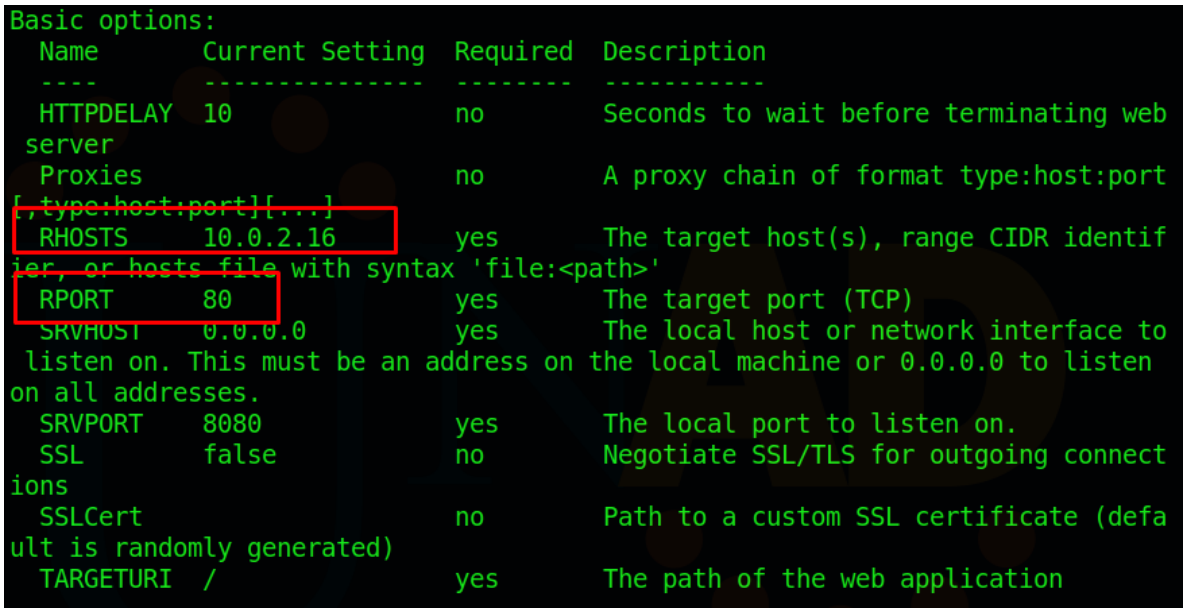
Ilustración 17. Uso del exploit rejetto_hfs_exec



Fuente: Propia de la actividad

Se abre el programa metasploit y se usa el modulo correspondiente en este caso rejetto_hfs_exec

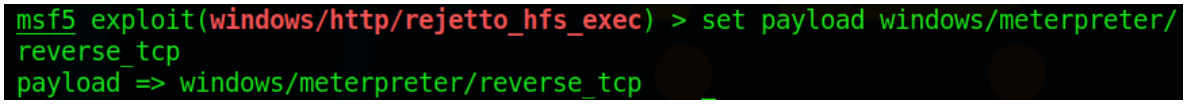
Ilustración 18. Configuración de parametros



Fuente: Propia de la actividad

Se procede a configurar cada campo de acuerdo al host identificado. Para este caso será RHOST y RPORT

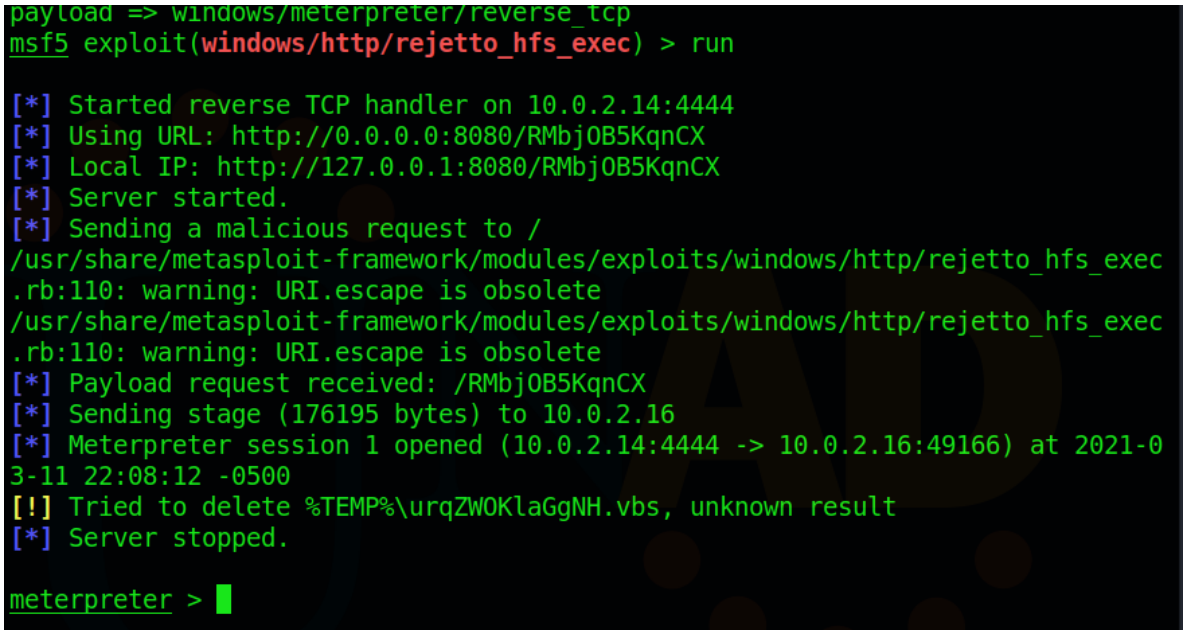
Ilustración 19. Carga de payload de ejecución



Fuente: Propia de la actividad

Se procede a cargar el Payload que permitirá realizar la ejecución del exploit esto con el comando set payload windows/meterpreter/reverse_tcp

Ilustración 20. Ejecución de Exploit

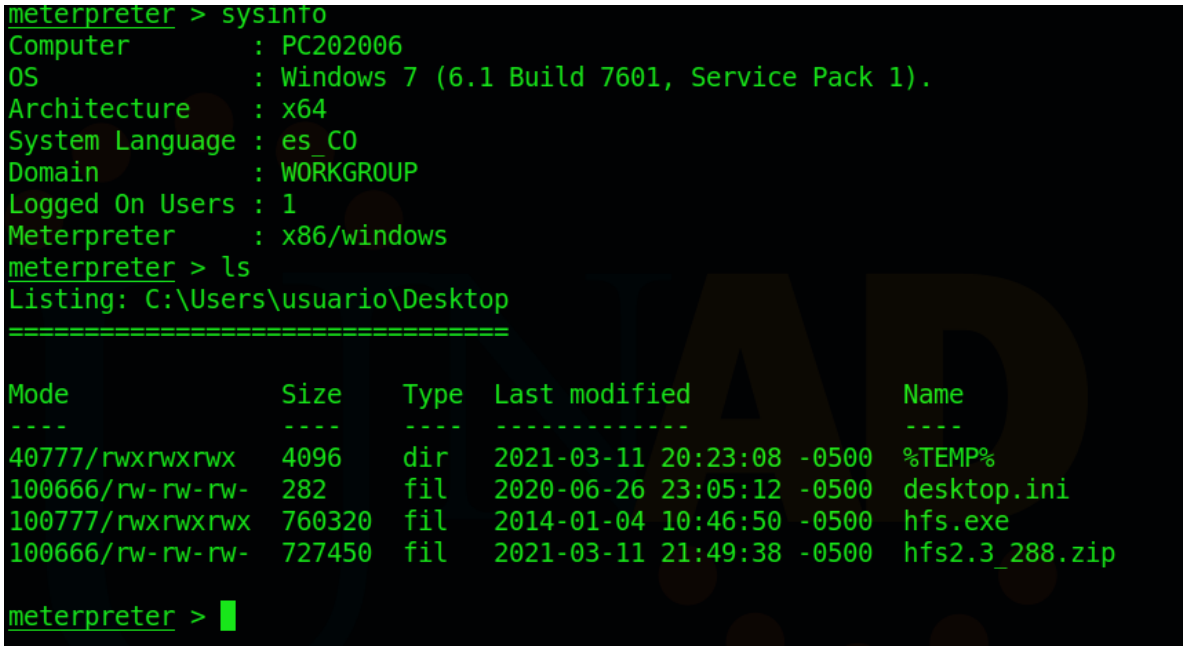


Fuente: Propia de la actividad

Se procede a lanzar el exploit con el comando run

Ya con el meterpreter habilitado se procede a realizar escalamiento de privilegios, información de servicios entre otros.

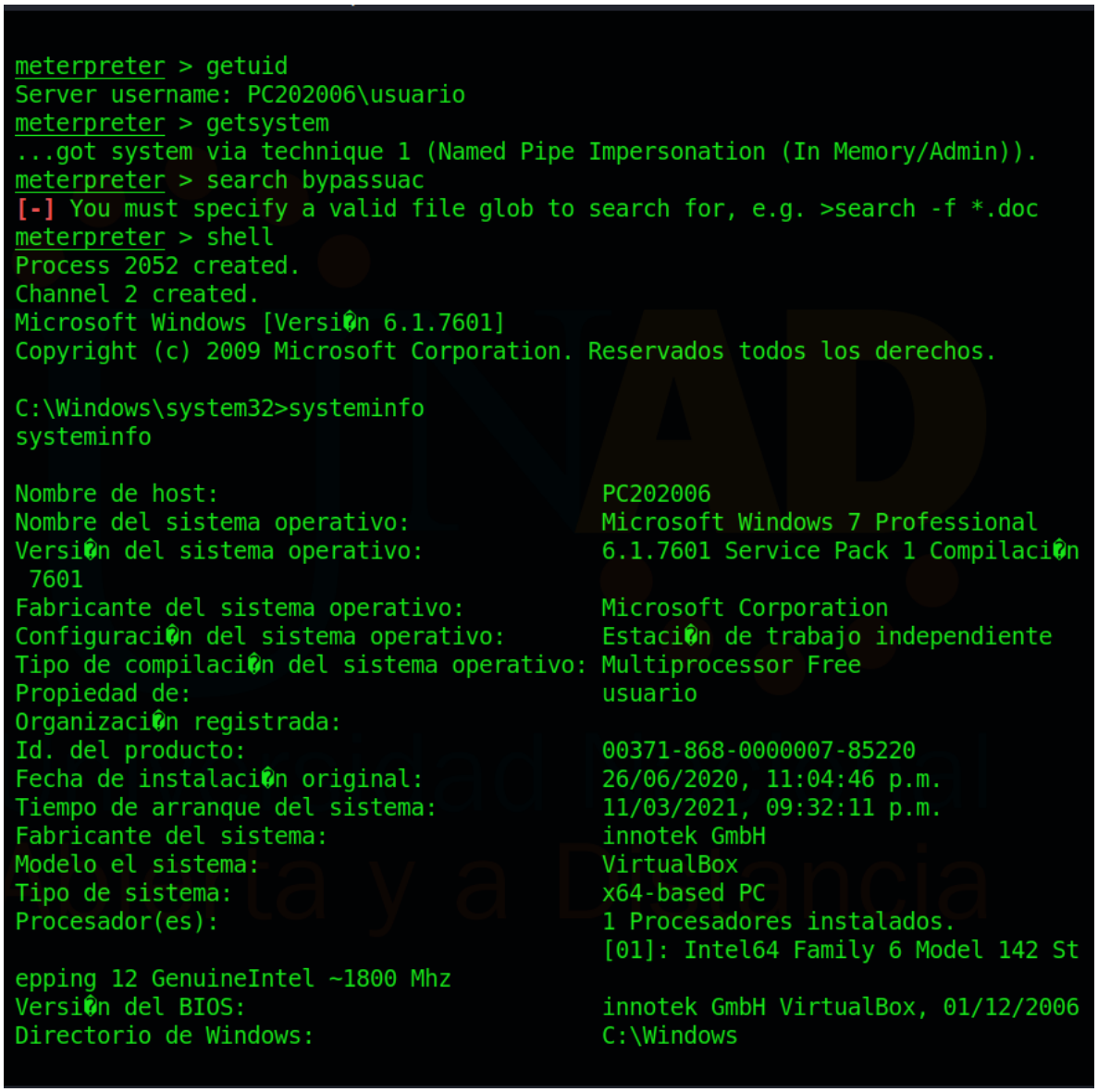
Ilustración 21. Información del sistema



Fuente: Propia de la actividad

Desde la consola de meterpreter se procede a revisar la información de la maquina que se accedió con el comando sysinfo, además con el comando ls podemos listar los directorios que tenemos disponibles desde la ruta o ubicación donde esta ubicado.

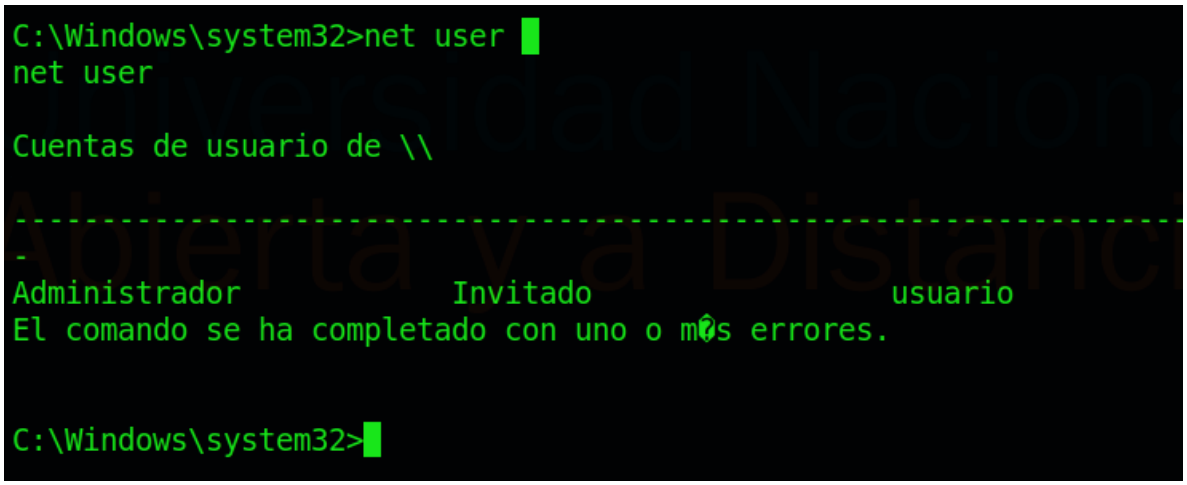
Ilustración 22. Shell de windows ejecutando



Fuente: Propia de la actividad

Se ejecuta desde el meterpreter el comando getuid para revisar el nombre del usuario actual, Se procede a acceder al ambiente windows desde el Shell ejecutando el comando Shell y como tal revisar la información del sistema con los comandos windows para este caso systeminfo

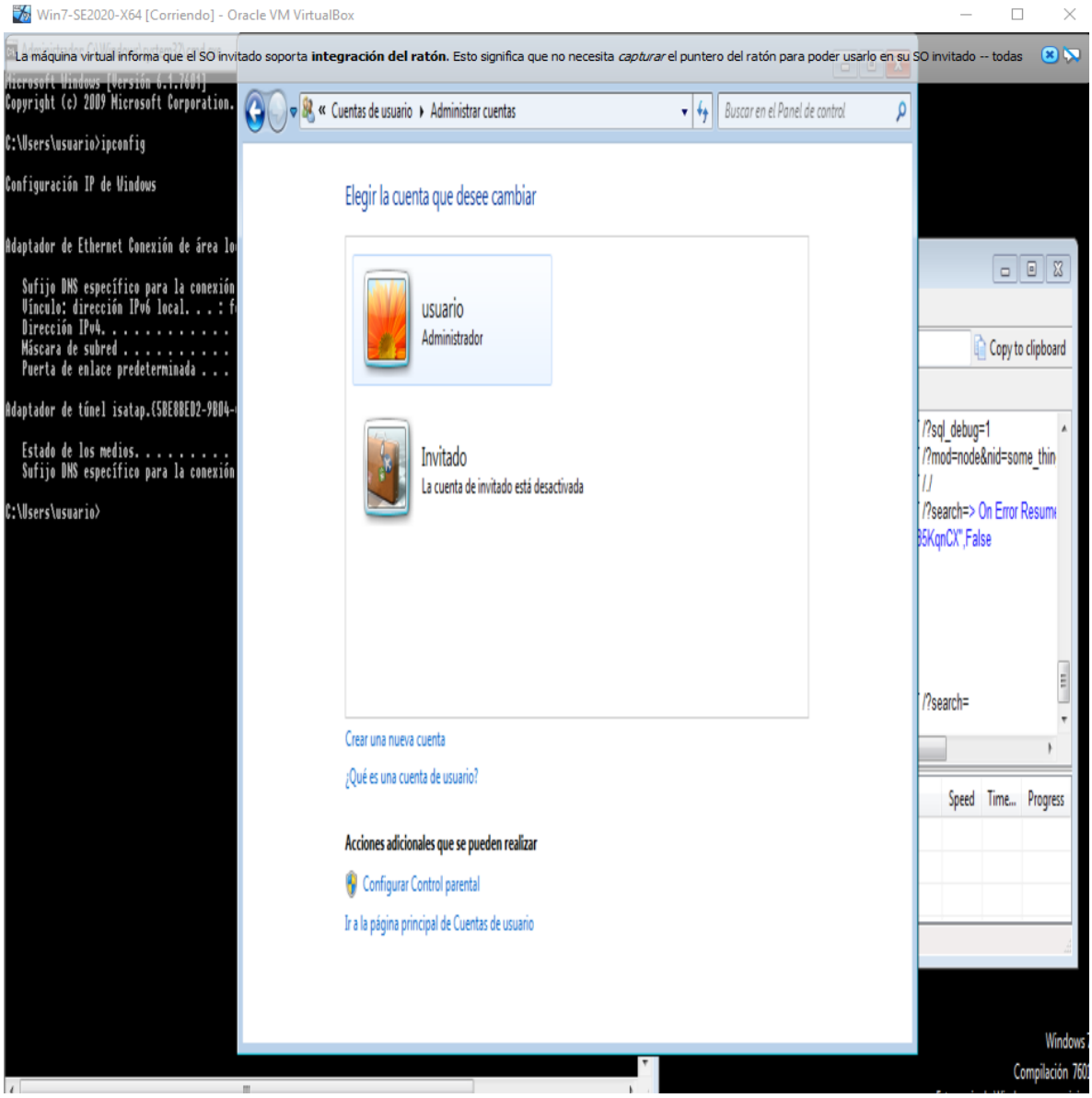
Ilustración 23. Usuarios disponibles en windows



Fuente: Propia de la actividad

Se procede a listar los usuarios desde la shell de windows abierta con el comando net user

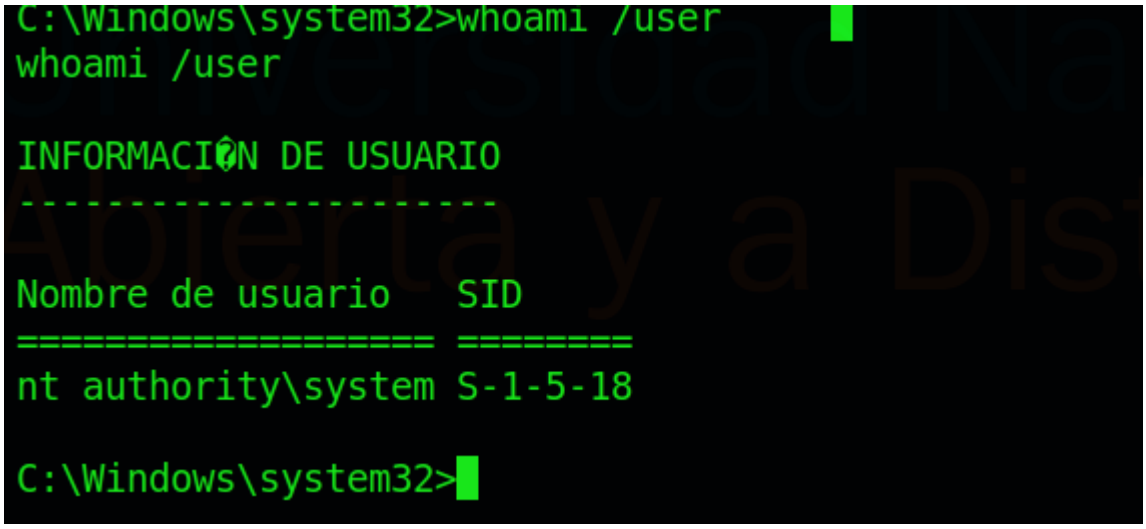
Ilustración 24. Usuarios de Windows7 X64



Fuente: Propia de la actividad

Se verifican los usuarios de windows

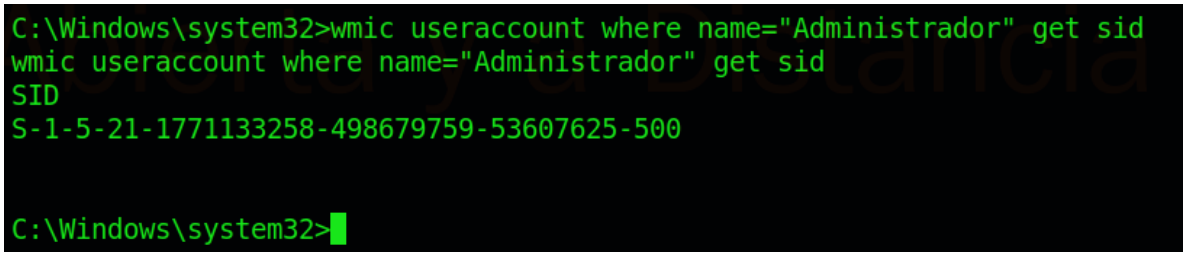
Ilustración 25. Identificador de usuario



Fuente: Propia de la actividad

Se observa la información de usuario y sus privilegios con el comando whoami /user esto permite observar tanto el nombre del usuario como lo muestra el sistema además del SID identificador

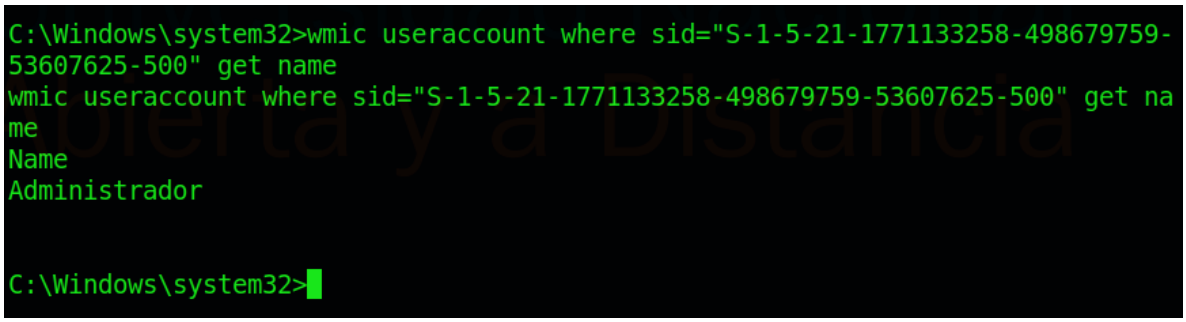
Ilustración 26. Obtención de identificador del usuario administrador



Fuente: Propia de la actividad

Se procede a sacar el SID del usuario administrador usando el comando wmic useraccount where name=”Administrador” get sid

Ilustración 27. Comprobación de SID del usuario administrador



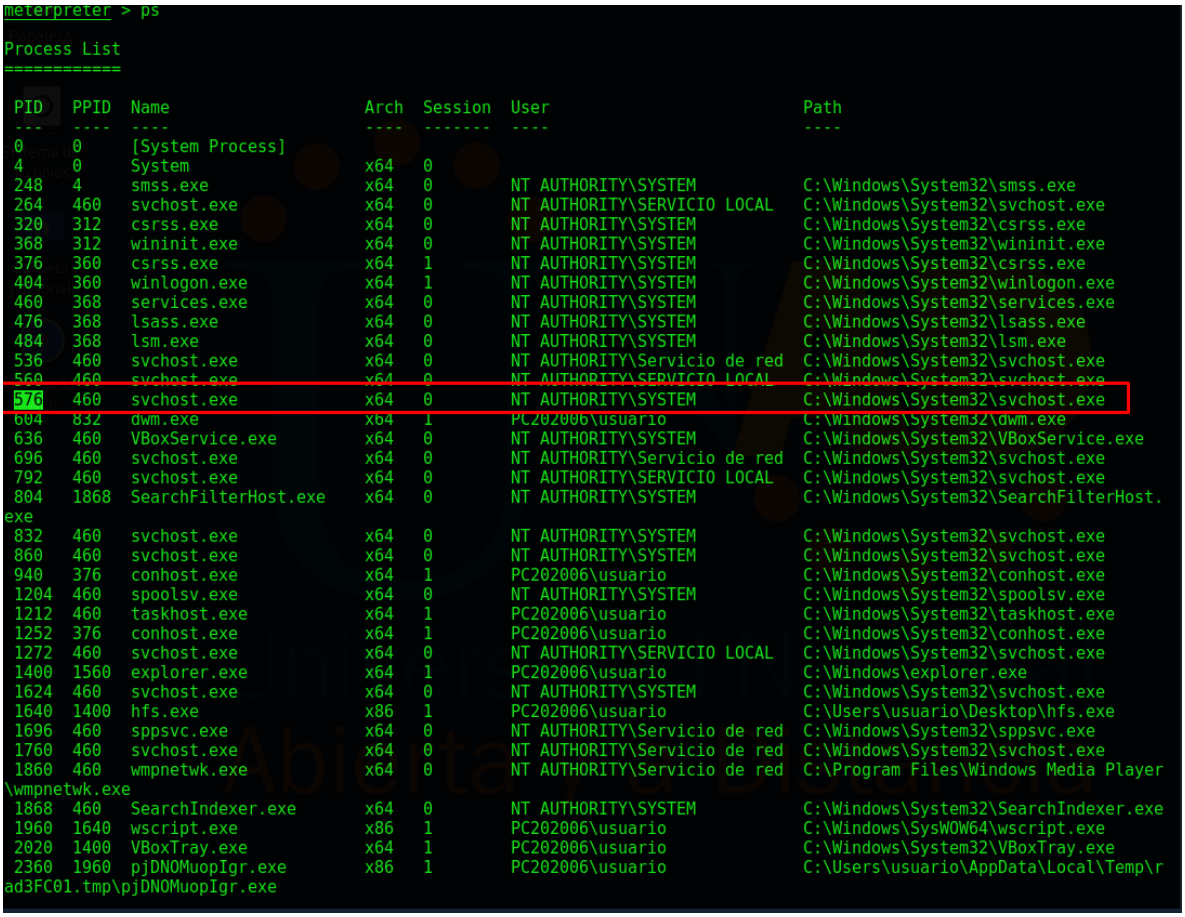
Fuente: Propia de la actividad

Se verirfica el SID obtenido dando una comprobación de identificador permitiendo mostrar a que usuario pertenece, esto nos permitirá usar dicho SID para acceder como usuario administrador

4. PostExplotación

   Se procede a extraer y capturar las credenciales realizando escalada de privilegios y obtrención de hashes

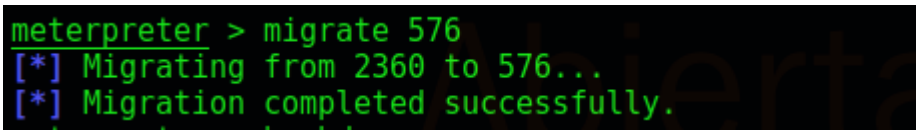
Ilustración 28. Verificación de procesos



Fuente: Propia de la actividad

Se procede a revisar los procesos desde el meterpreter con el comando PS. Aquí es necesario aclarar que debemos buscar el process ID de acuredo al usuario del sistema, en este caso será el PID 576

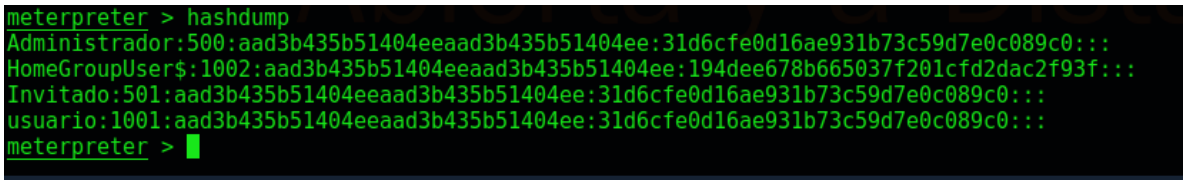
Ilustración 29. Migración de proceso



Fuente: Propia de la actividad

Una vez identificado se procede a migrar el proceso de svchost.exe que se encuentra con el identificador 576 usando el comando migrate

Ilustración 30. Obtención de credenciales de acceso de todos los usuarios



Fuente: Propia de la actividad

Una vez realizada la migración del PID ahora se procede a obtener el hash de las credenciales ejecutando hashdump donde podemos encontrar el respectivo hash de contraseña del usuario en cuestión el Administrador.

4. RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN

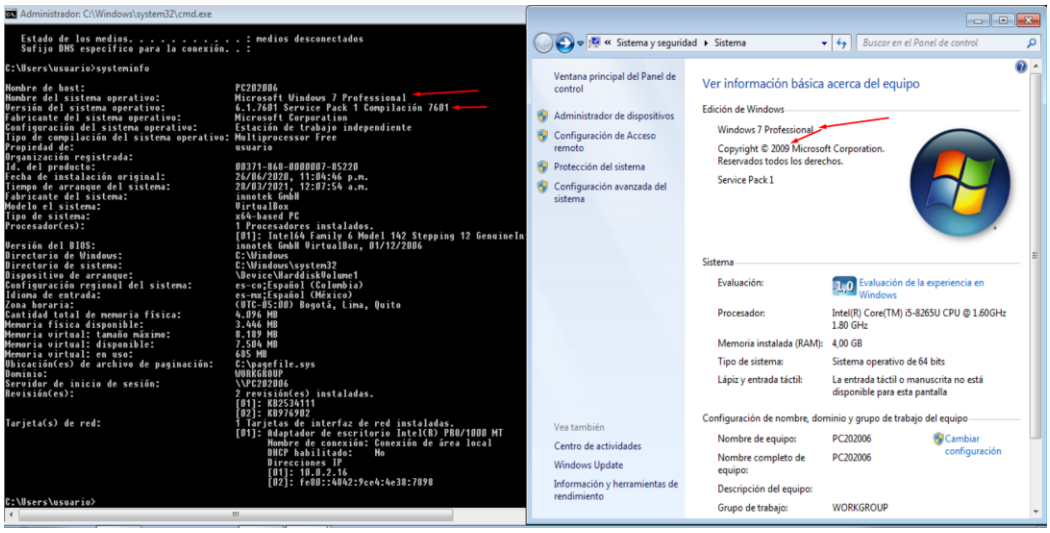
Basado en la metodología impartida por el NIST[3] encontramos un framework de adaptación basado en Identificar, Proteger, Detectar, Responder y Recuperar.

Identificar el vector y tipo de ataque que se está efectuando. En lo posible contener su origen y por ende activar los protocolos de bloqueo. Desarrollar un entendimiento de la organización para gestionar el riesgo de ciberseguridad en sistemas, gente, activos, informacióny capacidades.

- Revisión Estado actual maquina Windows 7 X64
- Levantamiento de Información

[3] NIST Framework, (National Institute of Standards and Technology –(Computer Security Incident Handling Guide) Tomado de https://www.nist.gov/cyberframework Link activo al 20/03/2021

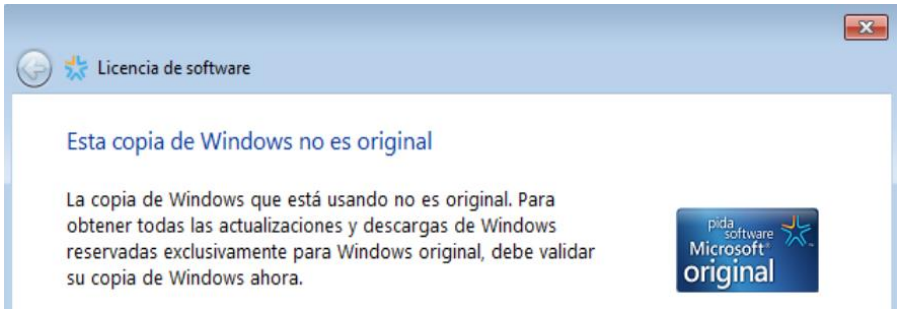
Ilustración 31. Versión del sistema operativo obsoleta



Fuente: Propia de la actividad

Se verifica la información de la maquina Windows 7 X64 y se encuentra que la versión del sistema operativo actual es obsoleto.

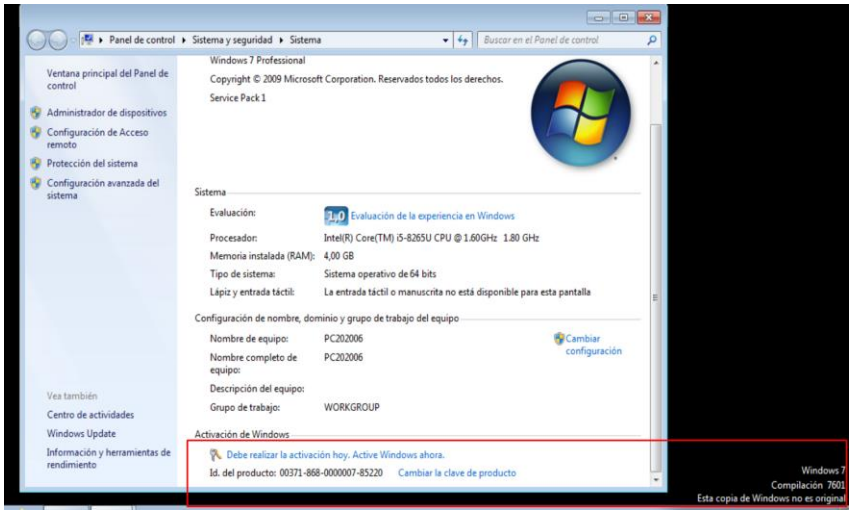
Ilustración 32. Copia de Sistema Operativo no original



Fuente: Propia de la actividad

Se encuentra que el sistema operativo no está licenciado

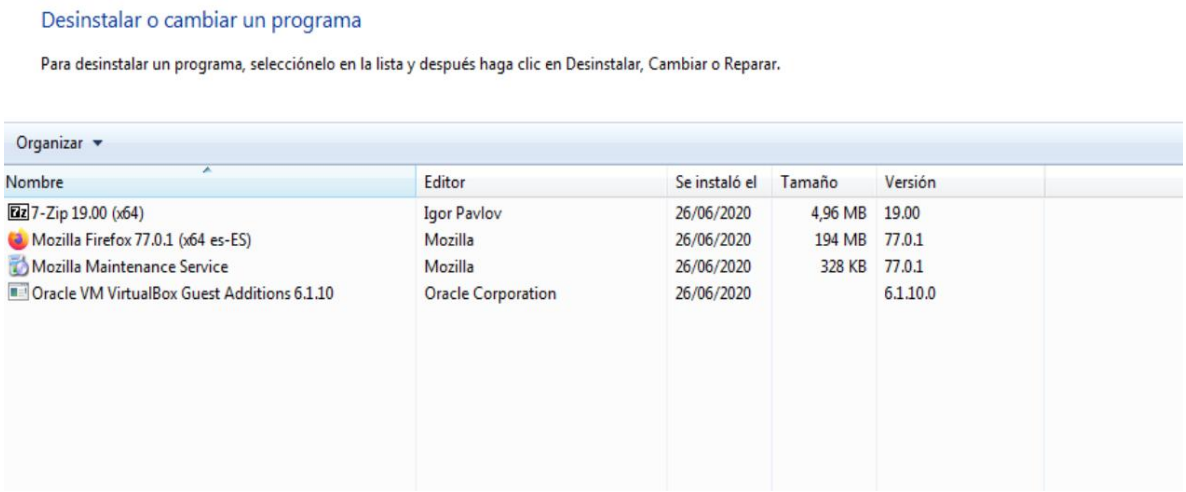
Ilustración 33. Sistema operativo sin licencia



Fuente: Propia de la actividad

Como tal la licencia tiene un tiempo de expliración además de la marca de agua indicando que el software no es original.

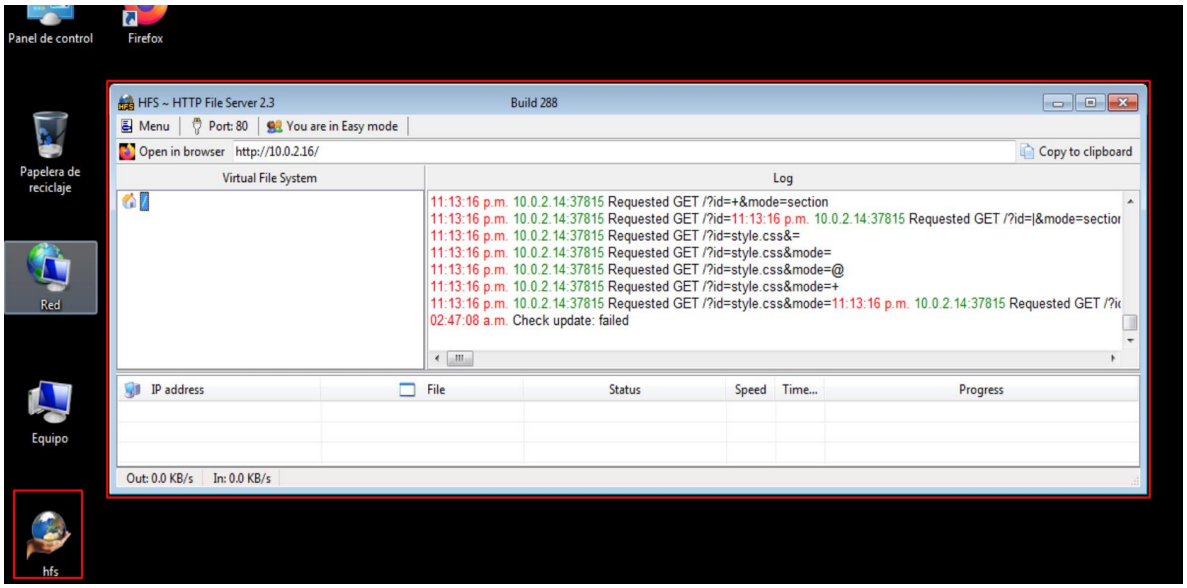
Ilustración 34. Software existente.



Fuente: Propia de la actividad

Se verifican los permisos del usuario actual y se confirmna que el usuario puede instalar software sin supervisión

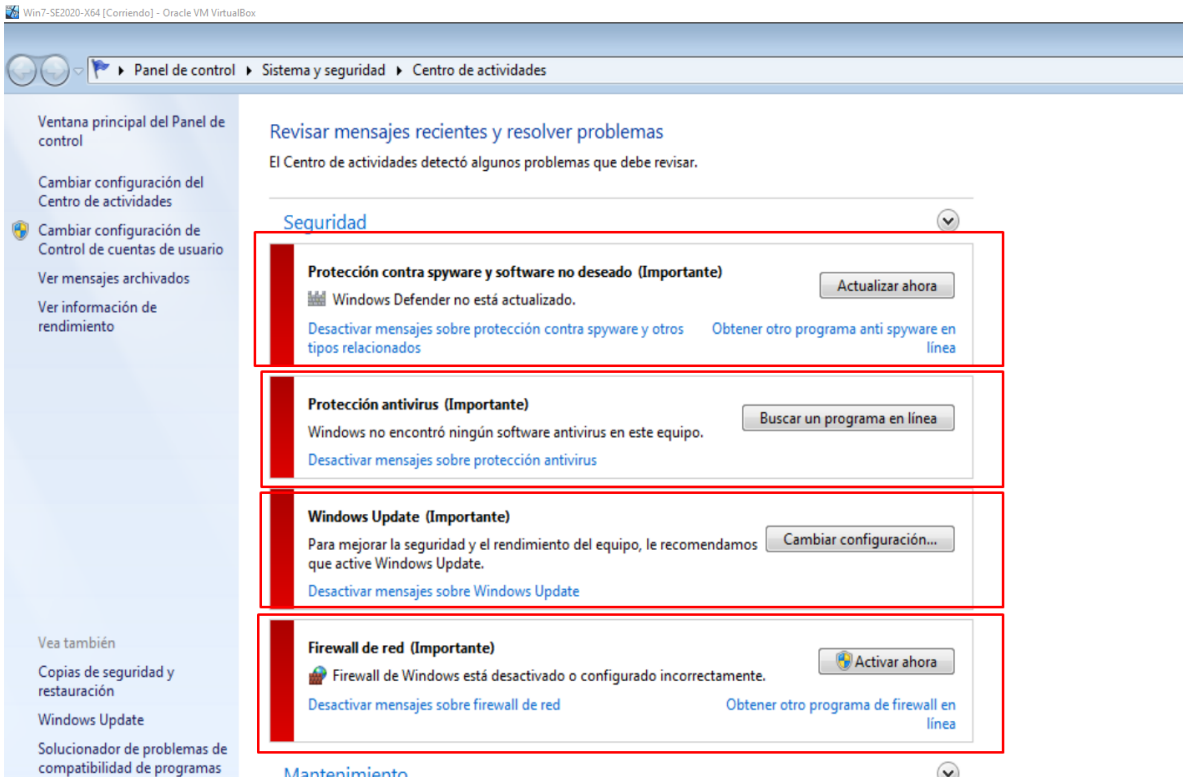
Ilustración 35. Software instalado sin supervisión



Fuente: Propia de la actividad

Bajo esta información se observa la instalación del software HFS el cual permite explotar el vector de ataque y materializar la vulnerabilidad.

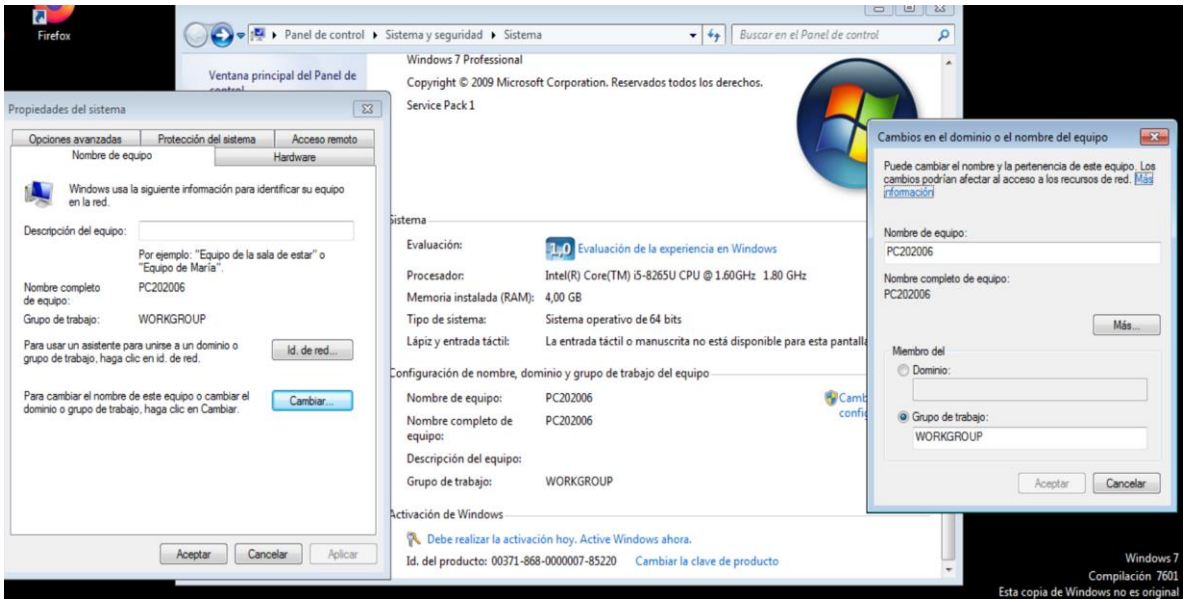
Ilustración 36. Seguridad debil o nula en la maquina



Fuente: Propia de la actividad

No hay software de protección antimalware, ni de firewall local sobre el equipo además de la falta de actualizaciones sobre el sistema operativo

Ilustración 37. No pertenece a un dominio.



Fuente: Propia de la actividad

Se verifica que el equipo está en un grupo de trabajo sin cumplir o adoptar políticas. Si el equipo es corporativo debe estar asociado a políticas de una organización, asociado a un dominio.

Ilustración 38.NIST: Proteger

Fuente: Nist Framework

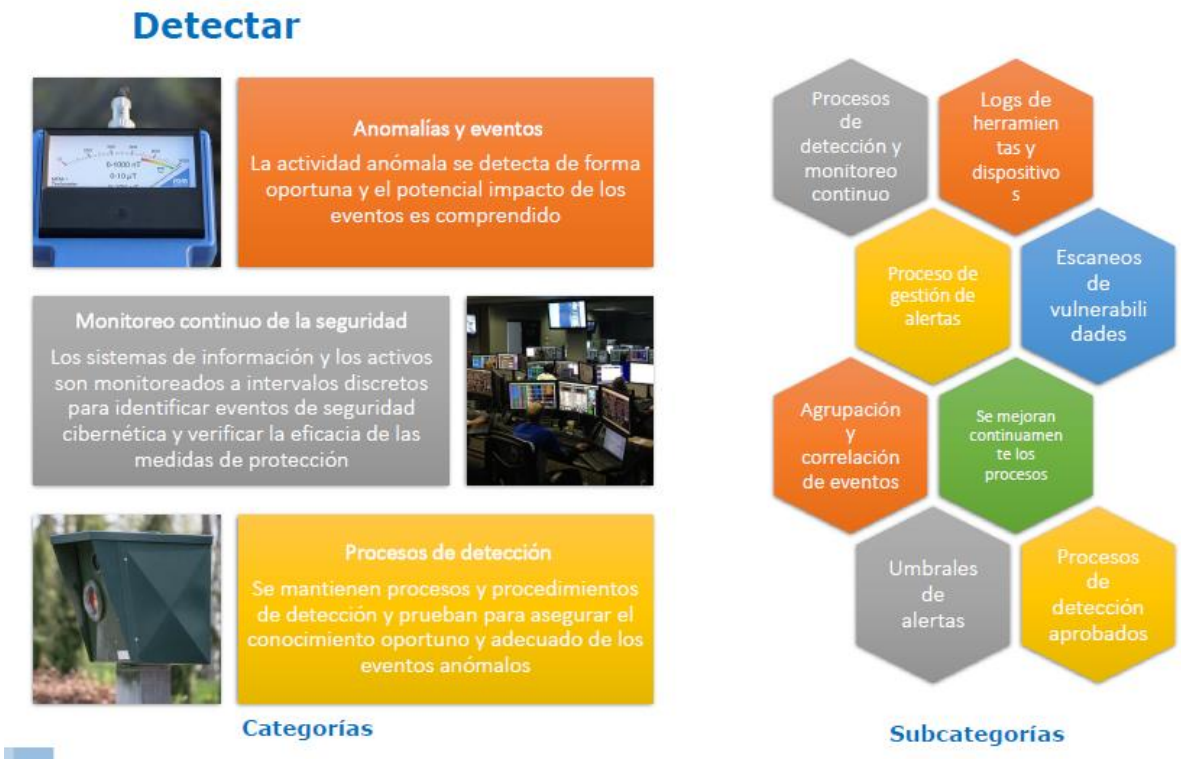
Proteger el entorno de Red corporativa, los demás activos que puedan ser afectados. Desarrollar e implementar las medidas de protección adecuadas para asegurar la continuidad y entrega de servicios críticos.

Lo primero que se debe tener presente es el tipo de activo que está siendo atacado, esto permite la clasificación e impacto sobre el core de negocio que se va a contener, seguido a ello en lo posible aislar la maquina que se identifique como principal y en su defecto proceder a realizar un levantamiento de información sobre esta. Realizar restauración de backup, analizar el tipo de ataque efectuado y realizar la verificación o hardenización de esta. De acuerdo al ataque efectuado realizar una correspondiente gestión del incidente presentado, dejarla en seguimiento y aplicar las medidas correctivas.

- Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización:

- Software actualizado y licenciado (GPL, Privado)
- Protección mínima en antivirus
- Pertenencia a un dominio con políticas de trabajo asociadas al tipo de usuario
- Desde la administración de red se sugiere la segmentación de equipos de acuerdo al área de trabajo, criticidad de la información y operatividad.
- Obligar el cambio periódico de contraseña (cada 3 meses)
- Identificar y verificar los puertos exclusivamente necesarios para la operación del servicio, aquellos puertos que no son requeridos, bloquear o restringir su acceso. Se recomienda verificar las reglas en el firewall para poder mitigar cualquier conexión o tráfico que salga por cualquier puerto no autorizado de los servidores productivos o u otras máquinas de producción. Filtrar el tráfico entrante sobre los servicios que operan dichos servidores
- Se recomienda un sistema de backup controlado para la información con sus respectivas copias (Diferente a la ubicación actual)
- Monitoreo y supervisión sobre los logs de eventos
- Concientización y formación
- Procesos y procedimientos para la protección de la información
- Protección perimetral Firewall, IDS, IPS, SIEM, EDR etc.

Ilustración 39. NIST: Detectar



Fuente: Nist Framework

Detectar posibles anomalías, fugas de información, escalamiento transversal/vertical y usuarios afectados además de los grupos de información con los que pueda replicarse. Desarrollar e implementar actividades apropiadas que permitan identificar la ocurrencia de un evento de ciberseguridad.

Fuente: Nist Framework

Responder de manera inmediata a tal punto de no poner en riesgo la organización en este caso ejecutando actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente. Desarrollar e implementar actividades apropiadas que permitan tomar acciones sobre un incidente de ciberseguridad detectado.

Ilustración 40. NIST: Recuperar

Fuente: Nist Framework

Recuperar el estado original de los activos de información minimizando las perdidas, restaurando de manera oportuna los sistemas o activos afectados. Desarrollar e implementar planes de resiliencia y para restaurar las capacidades o servicios que se hayan visto afectados debido a un ciberincidente

5. CONCLUSIONES PARA LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD

- Se debe estar alerta, preparado y manejar un nivel de resiliencia que permita dar una correcta atención a los posibles incidentes que se puedan generar.
- El proceso de manejo, gestión y atención adecuada permitirá mantener la organización a flote y su reputación alta.
- Lecciones aprendidas y modelos se seguridad maduros con el tiempo irán fortaleciendo nuestras actividades a nivel de ciberseguridad.
- Conocer las normas y leyes de acuerdo a cada país, regular y adoptar las medidas correspondientes, en general existen estándares de seguridad a nivel país para adaptarlas acorde al Core de negocio.
- Así mismo los principios y valores de cada profesional se deben impartir en cada aspecto que se encuentre, siempre prevalecer la ética profesional.
- Las medidas de seguridad en ambientes empresariales se deben tomar en serio desde la implementación del hardware y software mínimo como las políticas de seguridad asociadas a la seguridad de la información.
- Una constante actualización a nivel de software, hardening a los dispositivos y herramientas nuevos y capacitación además de sensibilización al personal hacen parte de una cultura segura.
- Abarcar la ciberseguridad a todas las áreas del negocio
- La detección y pronta reacción a ciberataques permitirá proteger la Confidencialidad, Integridad y Disponibilidad de la Información.
- El actuar y las responsabilidades como profesionales a que están atadas las diferentes actividades tienen un acto ético y a su vez legal y social para con la comunidad.
- El desconocimiento de las diferentes leyes no exime de responsabilidad de cualquier acto de tema legal que se imparta basado en las consecuencias de los actos de cada persona
- La importancia de cumplir con las medidas mínimas de seguridad permitirá reducir la brecha de ataque

6. LINK DE VIDEO:

https://youtu.be/QmSCSOjQOBc

7. BIBLIOGRAFÍA

- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J. y Sweetnam, J. (2020), Integridad de datos: detección y respuesta al ransomware y otros eventos destructivos, publicación especial (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [en línea], https://doi.org/10.6028/NIST.SP.1800-26 (Consultado el 20 de marzo de 2021)
- Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. Recuperado de: https://www.cisecurity.org/cis-benchmarks/
- COPNIA, Código de ética para el ejercicio de la Ingeniería en general y sus profesionaes afines y auxiliares. [En línea] disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf
- Derecho penal en la red. Convención americana sobre derechos humanos, entro en vigor el 18 de julio de 1978, p. 4 [En línea] disponible http://www.derechopenalenlared.com/legislacion/pacto-san-jose-costa-rica.pdf. (s.f.).
- Grammatech. (2016). Software Hardening. 2016, de grammatech.com. [En línea] disponible: https://www.grammatech.com/software-hardening.
- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27)Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
- HERNÁNDEZ LOTERO NATALIA, Clasificación De Los Datos Personales E Implicaciones Legales, [En línea] disponible en https://repository.upb.edu.co/bitstream/handle/20.500.11912/3595/Clasificaci%C3%B3n%20de%20los%20datos%20personales%20e%20implicaciones%20legales.pdf?sequence=1
- INCIBE. Instituto nacional de ciberseguridad, ¿Qué es el pentesting? Auditando la seguridad de tus sistemas [En línea] España https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements: Online: https://www.iso.org/standard/54534.html

- Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf
- Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63) Recuperado de: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf
- OPENWEBINARS , Que es un Payload, [En línea] disponible en https://openwebinars.net/blog/que-es-payload/.
- Velliadou, D. , Tasidou, K. , Antoniadis, K. , Assael, M. , Perkins, R. and Huber, M. (2021), Reference Correlation for the Viscosity of Xenon from the Triple Point to 750 K and up to 86 MPa, International Journal of Thermophysics, [online], https://dx.doi.org/10.1007/s10765-021-02818-9 (Accessed March 20, 2021)
- WEEBLY.COM, ESTUDIO DE CASO Nº 3Seguridad Militar: “Seguridad de Personal” [En línea] disponible en https://curso105.weebly.com/uploads/5/4/8/8/54887311/estudio_de_caso_n%C2%BA_3.pdf